

Phoenix Contact GmbH &Co

5

**Process and device for the packet-oriented
transmission of security-relevant data**

Description

10

The invention concerns a process and devices for the packet-oriented transmission of security-relevant data.

15

Particularly in the transmission of security-relevant data over an unsecured medium such as, for example, a common network and/or bus system, such data is usually added a high-grade redundancy so that almost all statistical and systematic errors of the overall transmission system do not have any negative impact on the integrity of the data whereby compliance to high security-related requirements with respect to the communication between individual network or bus users is achieved.

20

As a rule this is done by the extension of the security-relevant data by a data securing value which is generated on the basis of the security-relevant data and added to the security-relevant data of a data packet to be transmitted in accordance with the underlying protocol.

25

The patent application DE 100 65 907 A1 open to public inspection, for example, reveals a process that is based on

30

the generally known principle of 'redundancy cross
referencing'. In this, at the side of the sender, security-
relevant data supplied over one or two channels, depending on
the type of application, is edited in a twofold manner, i.e.,
5 in two data packets, and independently from each other using
redundant information and then sent to the recipient over
separate connections or time-delayed one after the other over
a single connection. Depending on the application the data
content of one of the two edited security-oriented data
10 packets may also show inverted data or other additional
interleaving to recognize, for example, also systematic
errors in the senders, receivers and/or other units involved
in the transmission of the data. In addition to this, the
mentioned application open to the public provides for a
15 cross-reference verification of the two edited data packets
for correctness at the side of the sender and/or receiver by
reviewing the respectively added redundancy.

The complete state-of the-art security-oriented message is
20 then, for example, structured as shown in the attached hereto
Fig. 3 whereas this security-oriented message comprises two
data packets 3 and 3'. According to Fig. 3 the security-
relevant data contain - besides the user data as such -
additional control data whereas each of the data packets 3
25 and 3' contains this data with the same information content,
but differently coded. In addition to this, each data packet
3 or 3' contains a block of redundant information
(CRC or CRC) generated on the basis of the security-relevant
data.

30

A substantial disadvantage of this principally known state-
of-the-art process, however, is to be found in particular in
the unfavorable relation between the user data length and the
overall data length which even gets worse with a decreasing

volume of user data to be transmitted per data packet as is, for example, the case with an interbus.

One aim of the invention is thus the task to provide a new
5 and - in relation to the state of the art described above -
enhanced way for the packet-oriented transmission of
security-relevant data granting a considerably enhanced rate
of user data and ensuring a high-quality protection against
statistical and systematic errors in an unsecured medium.

10 The solution of the task according to the invention is in a
very surprising manner already given by a process with the
elements of claim 1, a device with the elements of claim 10,
and a transmission system with the elements of claim 19.

15 Advantageous and/or preferred types of execution or further
developments are subject to the corresponding claims.

20 According to the invention it is thus provided for the
packet-oriented transmission of security-relevant data,
particularly under application of at least one transmission
system including a parallel and/or serial network and/or bus
system with at least one user connected to it that the
security-relevant data and a redundant information based on
25 the security-relevant data are transmitted in different
packets.

It is thus of considerable advantage that a high protection
against statistical and systematic errors, particularly in
30 the case of a transmission over an unsecured medium, can be
guaranteed along with a considerably enhanced rate of user
data.

For practical reasons, the invention thus provides for the
35 provision of a device for the packet-oriented transmission of

security-relevant data between at least two network and/or bus users that has means arranged on the side of the sender for the packet-oriented embedding of security-relevant data and allocated redundant information into different packets
5 and/or means arranged on the side of the receiver designed to verify an error-free transmission of security-relevant data on the basis of security-relevant data and allocated redundant information being embedded in different packets.

10 The invention thus furthermore allows that only means for the generation, transmission and verification of a single redundant information unit pertaining to each security-relevant data unit are required which leads to a considerable simplification with respect to the processing of data ,
15 particularly of security-based input and output devices or input and output users of a transmission network and/or bus.

To ensure that essentially all statistical and systematic errors in the transmission system are identified, an encoding
20 device allowing the encoding of the relevant redundant information is provided for.

As a particularly preferred further development, the invention proposes to use a data protection value for the
25 redundant information including a check sum calculated above the security-relevant data.

By using, for example, a polynomial such a check sum can be chosen so that in a particularly preferred way, each of the
30 possible check sums results from one of the possible combinations of the security-relevant data.

The invention thus guarantees an extremely good protection from error bursts as well as from inversion errors with

respect to individual components of the security-oriented message to be transmitted as a whole.

According to practical further development, the means
5 arranged on the side of the sender for embedding are
allocated driver-like means for the generation of redundant
information that show the same number of bits as the
security-relevant data to be transmitted. The invention can
thus be essentially used in an application-specific way with
10 essentially all currently known networks and/or bus systems
as, for example, Interbus, Ethernet, Profibus or CAN.

With the transmission of security-relevant data and allocated
redundancy in separate packets according to the invention it
15 is therefore possible to set a high Hamming distance.

As the invention consequently moreover allows to ensure -
even for a small volume of user data - high dynamics already
on the basis of a single changing bit, a particularly good
20 identification of systematic errors, especially of unsecured
network and/or bus users including switches, routers,
amplifiers, gateways, system couplers and/or a master can
also be guaranteed for the transmission of the data.

25 Depending on the application-specific used serial and/or
parallel networks and/or bus systems the invention moreover
provides for the fact that the security-relevant data,
comprises - besides the user data as such, i.e. in particular
input/output data and/or other safe process data - further
30 data, in particular check and/or control data.

It is further intended to transmit the packets with the
allocated to each other security-relevant data and redundant
information parallel or serially and/or several packets
35 within a predefined (superset) frame structure so that the

invention can be used with the most different applications and/or fields of application. Particularly in the latter case, it is further preferentially proposed to jointly transmit security-relevant data and the allocated redundant information generated on the basis of such data within the predefined structure of a (superset) frame structure to simplify the implementation of the provision of means to read out and verify the security-relevant data and allocated redundant information on the side of the receiver particularly with respect to the allocation functionality.

If the packets with the allocated to each other security-relevant data and redundant information are transmitted separately, a preferred further development provides that the data packets to be transmitted comprise an addressing block and/or an identification code for their logical allocation. As far as the practical execution is concerned, such an addressing and/or identification code is embedded in the data packets to be transmitted by means adapted to the specific application on the side of the receiver based on the respectively used transmission format and verified by correspondingly designed readout means on the side of the receiver to achieve a logical allocation of data packets with contents allocated to each other in order to verify an error-free transmission.

Depending on the invention's field of application which may be found, for example, in the fields of building control technology, process industry, manufacturing industry, passenger transportation and/or the operation of automation plants, and based on the individual structure of the respective network and/or bus system which, in particular, shows a ring-, line-, star- and/or tree-shaped structure, the invention allows the beneficial integration of the aforementioned means implemented on the sides of the sender

and receiver in accordance with the invention into essentially every user device, i.e. particularly into master and/or slave users.

5 In the following, the invention is described with a preferred design example with reference to the enclosed figures.

The following shall be valid for the enclosed figures:

Fig. 1 shows the invention-based structure of data packets
10 for the packet-oriented transmission of security-relevant data.

Fig. 2 shows a further invention-based structure to illustrate the considerably enhanced identification of systematic errors.

15 Fig. 3 shows the structure of a security-oriented message according to the current state of the art.

Referring to Fig. 1, for the provision of a packet-oriented transmission of security-relevant data with a guaranteed high
20 rate of user data and, at the same time, at a high-level of protection against statistic and systematic errors, an example for a security-oriented message comprising two data packets one and two to be transmitted according to the invention is shown.

25 According to the invention, a security-oriented message of a security-relevant data set - as shown in Fig. 1 - principally comprises at least two separate data packets 1 and 2 whereas one data packet 1 comprises security-relevant data, and
30 another data packet 2 comprises allocated redundant information.

Based on this structure in accordance with the invention it is ensured that for a transmission of security-relevant data
35 also via an unsecured medium, i.e. essentially via a bus

and/or network system which does not comply with security-oriented standards and/or comprises unsecured system users that essentially all statistical and systematic errors are identifiable.

5

In a data transmission, statistical errors are particularly based on external interference and/or electrical effects, whereas systematic errors are usually caused by software- and/or hardware-based errors of senders, receivers and/or
10 other devices forwarding the data as, for example, switches, routers, amplifiers, gateways and/or system couplers that are located along the transmission path.

Negative effects of such causes on the integrity of security-
15 relevant data can therefore - as further described in the following - be essentially completely excluded.

The data packet illustrated in Fig. 1 comprises - as security-relevant data - a protocol- and/or application-
20 specific user data block 11 and, in the present example, a check data block 12.

Depending on the application, such user data 11 is provided on the side of the sender particularly by sensors, actuators
25 and/or control devices over one or two channels and transmitted to a defined receiver as, for example, an actuator or actuating drive of a protective barrier on the basis of the overall structure of the transmission system which may comprise ring-, line-, star- and/or tree-shaped
30 network and/or bus structures. Such user data 11 therefore often comprise pure input/output data. Fields of application of transmission systems where such user data 11 partly or to its full extent represents security-relevant data are consequently particularly found in the fields of the

manufacturing industry, public transport, fuel engineering, process industry, or building control technology.

In addition to the pure input/output data 11, check data 12
5 and/or additional secure or insecure data as, for example, control data, or a sequence number 12b as shown in Fig. 2 are often generated for process control. This additional data essentially enables, for example, the communication
10 participants to verify the proper function of other participants, especially via checking the transmission path over signal chains by exchanging the relevant check data blocks 12.

Data packet 2 completing the security-oriented message
15 comprises a redundant information 21 that is allocated to the information content of data packet 1, i.e. a data securing value 21 that is based on the user data 11 and the check data 12.

20 The data securing value 21 contained in data packet 2 is expediently a check sum CRC calculated over the user data 11 and the check block 12 which is generated on the side of the sender using adapted driver-like means, in particular a microprocessor or similar programmable circuit design, on the
25 basis of an error-checking algorithm, e.g. in the form of a generally known 'Cycle Redundancy Check'.

On the side of the receiver or at a defined processing location, the partial messages 1 and 2 are read out
30 particularly by slave users and/or a master user that are arranged depending on the application and then verified for an error-free transmission by checking the redundant information 21 with respect to the security-relevant data 11 and 12, before the security-relevant user data 11 is passed

on to the corresponding output users as, for example, an actuator to actuate the same.

As data packets to be transmitted principally always comprise
5 the same number of bits for protocol-specific reasons, the data packet 1 comprising the security-relevant data which in the present example is the user data 11 and additionally the check data 12, and the data packet 2 comprising the check sum 21, also have the same bit length n.

10 Consequently, the user data rate, i.e. the relation between the useful data length and the overall data length, of a security-oriented message structured according to the invention is considerably higher if compared to a security-
15 oriented message in which - as shown in Fig. 3 - each data packet 3 and 3' comprises both the security-relevant data, i.e. in particular the user data, and a data protection value based on the security-relevant data, whereas these two elements are differently encoded.

20 Based on the embedding of the security-relevant data 11, 12 and the redundant information 21 in two different data packets 1 or 2 it is only necessary to generate a data protection value 21, and the invention thus allows to save
25 one data protection value compared to the transmission of security-relevant data according to the state of the art (Fig. 3).

30 In order to additionally guarantee - besides the enhanced user data rate -, in particular with the transmission of a security-relevant data set comprising only a small volume of user data 11, a high-level of error protection for the sending and/or forwarding of security-relevant data by insecure slave users and/or an insecure master, the data

protection value 21 that consequently has an increased number of bits is particularly effective.

For this purpose, the data protection value 21, i.e. in particular the CRC polynomial or the error-checking algorithm used for the generation of a check sum, is preferably chosen such that each of the 2^n possible data protection values results from exactly one of the 2^n combinations of the security-relevant data. Therefore, both data packets 1 and 2 of the security-oriented message comprise essentially the same information, but are differently encoded.

For practical use, with an appropriate generation of the redundant information 21, a very high Hamming distance is therefore provided, and a good protection against error bursts, inversion of individual components of the data of the security-oriented message, and a good detection of errors, in particular also of systematic errors through the different partial messages 1 and 2 - as is detailed in the following with reference to Fig. 2 - is guaranteed.

Referring to Fig. 2, where a security-oriented message is made up of two data packets 1b and 2b each comprising 24 bits, the particularly good detection of systematic errors based on the invention becomes particularly clear. Here, the data packet 1b including the security-relevant data comprises two areas - one user data area 11b with 16 bits and one area 12b with 8 bits for the transmission of a sequential number.

If, for example, the process or input/output data to be secured, i.e. the user data 11b comprising 16 bits, do not change only the sequential number in the data area 12b' increments during an application. If the checking polynomial 21b has been appropriately chosen, a whole series of bits in the most different positions will change within the large

check sum 21 comprising 24 bits. These high dynamics of the messages thus allows the particularly easy detection of systematic errors in the devices forwarding the security-oriented messages guaranteeing the highest level of security.

5

Application-specific or based on the respectively used network and/or bus, the invention furthermore guarantees that the two partial messages 1 and 2 forming a security-oriented message are combined and jointly transmitted also within a predefined (superset) frame structure.

10

However, it must be principally pointed out that the two allocated to each other partial messages 1 and 2 may also be transmitted separately - for example, over separate connections or time-delayed over a single connection.

15

Furthermore, the invention guarantees that the allocated to each other partial messages 1 and 2 may also be embedded and transmitted within different predefined (superset) frame structures. For this purpose, it is for practical reasons provided that the individual packets are given an addressing block and/or an identification code for their logical allocation so that the readout, allocation and verification for an error-free transmission of received data can essentially also be performed independently from the time-related transmission and/or the type of transmission of the allocated to each other partial messages 1 and 2.

20

25

The invention thus allows the transmission of security-relevant data with a high user data rate over essentially any insecure media without giving up the required security. As an example the Interbus is referred to as a preferred transmission medium for the application of the invention where secure data with a low volume of user data is sent and/or forwarded by insecure users and/or the insecure master.

30

35